



# Department of Homeland Security Daily Open Source Infrastructure Report for 05 June 2007

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- The New York Post reports New York City pipeline security remains a problem, with the 40-year-old Buckeye pipeline that pumps jet fuel, heating and diesel oil, and gasoline into the city so exposed that anyone could simply walk up and touch the pipe. (See item [2](#))
- United Press International reports aviation security experts say the plot to blow up John F. Kennedy International Airport highlights the vulnerability of U.S. aviation system's infrastructure, which represents a vulnerable 'back door' to the nation's airports. (See item [11](#))

## DHS Daily Open Source Infrastructure Report *Fast Jump*

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *June 04, Reuters* — **Dominion to sell gas assets for \$6.5 billion.** Dominion Resources said on Monday, June 4, that it would sell most of its gas and oil exploration and production operations to two different companies for about \$6.5 billion as part of its plan to focus on its power business. Loews Corp., a conglomerate, will pay about \$4.03 billion for Dominion's gas assets in the Permian Basin in Texas as well as properties in Michigan and Alabama, while XTO Energy Inc., a natural gas producer, will pay about \$2.5 billion for the operations in the Rocky Mountains, Gulf Coast, San Juan Basin and Louisiana. The sale of these properties, which include 3.51 trillion cubic feet equivalent of proved natural gas and oil reserve as of December

31, is expected to close in August. The remaining properties earmarked last year for sale, largely in Oklahoma, will be marketed in a new process that will begin in July, Dominion said. Source: [http://www.nytimes.com/reuters/business/business-dominion-sales.html?\\_r=1&oref=slogin](http://www.nytimes.com/reuters/business/business-dominion-sales.html?_r=1&oref=slogin)

2. *June 03, New York Post* — **Pipeline security a problem.** The terror-targeted Buckeye pipeline snakes through miles and miles of city streets, coursing with millions of gallons of potentially lethal fuel each day — and is so exposed that a reporter could simply walk up and touch the pipe. For years, city residents have questioned the safety of the 40-year-old artery that pumps jet fuel, heating and diesel oil and gasoline into the city, and some have even cited the pipeline as a potential terrorist target. Three years ago, Rep. Vito Fossella (R-Brooklyn, S.I.) highlighted major security shortfalls surrounding a mostly submerged portion of the pipeline in Brooklyn, at the 65th Street rail yard on Fourth Avenue in Bay Ridge. Fossella showed that the security fence was consistently left open and that parts of the gate were sometimes missing. Security was so bad that homeless people have been seen roaming the yards. In 1985, the pipeline was punctured on Staten Island when a construction worker drove a backhoe into a valve. It was reported at the time that 35,000 gallons of gasoline had spilled into the street, as dozens of homes were evacuated and 200 firefighters responded.

Source: [http://www.nypost.com/seven/06032007/news/regionalnews/pipeline\\_security\\_a\\_joke\\_regionalnews\\_kaili\\_mcdonnough\\_georgett\\_roberts\\_and\\_patrick\\_gallahue.htm](http://www.nypost.com/seven/06032007/news/regionalnews/pipeline_security_a_joke_regionalnews_kaili_mcdonnough_georgett_roberts_and_patrick_gallahue.htm)

3. *June 02, Associated Press* — **Few gas stations comply with bill requiring power during evacuation.** A law went into effect Friday, June 1, that requires gas stations in Bay County, FL to be generator-ready in case of a power outage from a storm. Under the new law, gas stations within a half-mile of major evacuation routes must be prewired with a transfer switch and capable of operating fuel pumps, dispensing equipment and credit card payment equipment on generator power. They are not, however, required to have a generator on site. Companies that own ten or more retail gas stations in a single county must have one generator for every ten stations. Certain other companies that own multiple gas stations in the same region also are required to be able to operate on generators. Non-compliant station owners could be charged with a misdemeanor and fined up to \$500. According to the Florida Department of Environmental Protection, more than half the gas stations across the state that must comply with the new law are not in compliance. Of the 1,077 stations covered by the new requirement, 55 percent are believed to be in violation, according to the Department of Environmental Protection report released Thursday.

Source: <http://www.newsherald.com/headlines/article.display.php?a=1547>

4. *June 01, Associated Press* — **BP refinery repair delays force cut in Canadian oil intake.** Extended unit downtime at the BP PLC oil refinery in Whiting, IN, prompted the company to inform Canadian crude suppliers to the plant that it couldn't completely fulfill its purchase obligations, spokesperson Valerie Corr said Friday, June 1. The 410,000-barrels-a-day refinery, a major source of fuel supply to the Chicago market, has been operating at about half of its capacity since late March. Downtime for several major processing units has stretched from four to six weeks originally to months. Before crude processing rates fell in late March, Canadian crude made up about 20 percent of its throughput, or 82,000 barrels a day. Whiting is BP's largest U.S. refinery and the fifth-largest of all refineries in the United States.

Source: [http://biz.yahoo.com/ap/070601/bp\\_refinery\\_repair.html?.v=1](http://biz.yahoo.com/ap/070601/bp_refinery_repair.html?.v=1)

5. *May 31, Department of Energy* — **U.S. continues to lead the world in wind power growth.**  
The U.S. Department of Energy (DOE) Thursday, May 31, released its first Annual Report on U.S. Wind Power Installation, Cost, and Performance Trends: 2006, which provides a detailed and comprehensive overview of development and trends in the U.S. wind power market. The report concludes that U.S. wind power capacity increased by 27 percent in 2006; and that the U.S. had the fastest growing wind power capacity in the world in 2005 and 2006. In 2006, for the second straight year, the U.S. led the world by installing 2,454 MW of wind power capacity, enough to power the homes in a city the size of Philadelphia. The U.S. produced roughly 16 percent of the worldwide wind market, followed by Germany, India, Spain, and China.  
Report: <http://www.nrel.gov/docs/fy07osti/41435.pdf>  
Source: <http://www.energy.gov/news/5091.htm>

[\[Return to top\]](#)

## **Chemical Industry and Hazardous Materials Sector**

Nothing to report.

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

Nothing to report.

[\[Return to top\]](#)

## **Banking and Finance Sector**

6. *June 04, Australian Associated Press* — **Cyber crime fears grow as online banking grows.**  
The rapidly expanding ranks of people banking online has raised questions over whether consumers are armed to deal with the growing threat from cyber pirates. In the past year alone, the number of online bankers in Australia has swelled by 1.3 million, to 8.2 million, according to a survey by the Commonwealth Bank, accounting for 52 percent of the population. Security has become a major issue, with the Australian Competition and Consumer Commission (ACCC) saying the threat of fraud through attacks against online accounts is on the increase. In a submission to a current review of the Electronic Funds Transfer (EFT) Code of Conduct the ACCC found that customers who used electronic banking, such as Internet banking, faced severe threats from tech-savvy criminals. The Consumer's Telecommunications Network (CTN) believes many consumers are not adequately prepared to deal with the threat of such online attacks. In its November 2006 report, *Surfing on Thin Ice*, CTN said that although awareness of e-security threats may be reasonably high, consumer understanding of the threats and how to protect themselves against attack was lacking.  
Source: <http://www.smh.com.au/news/Business/Cyber-crime-fear-as-online-banking-grows/2007/06/04/1180809410102.html>

7.

*June 04, Finextra* — **Bank of Scotland customer data lost in the mail.** Bank of Scotland (BoS) is notifying more than 60,000 mortgage customers that a computer disc containing their personal information has been lost in the postal system. BoS says the disc contained names, addresses and dates of birth and mortgage account numbers for 62,000 mortgage customers, but it did not contain bank account details, PINs, passwords or transaction data. The bank had sent the disc via Royal Mail to a credit reference agency more than two weeks ago, but the data never arrived. BoS says "there is no suggestion that the disc was stolen" and it would appear to have been "misplaced in the post". BoS says it is "almost impossible" that any financial fraud could be committed with the data held on the disc, but it is offering affected customers free registration with CIFAS, the UK's fraud prevention service.

Source: <http://finextra.com/fullstory.asp?id=17000>

8. *June 04, ComputerWorld (New Zealand)* — **Cybercriminals outsource their dirty deeds.**

Once organized crime got involved in malicious activities on the Web, everything changed, Auckland University's IT security guru, Peter Gutmann, said at Computerworld's Security Briefing, held in Auckland, New Zealand, last week. Outsourcing, including anti-detection, is huge in today's commercial malware industry. When there is a problem, cybercriminals seem to find a solution. Not only are professional programmers contracted to write malicious code, spammers are hiring linguists to bypass filters, and phishers are employing psychology graduates to scam victims, he says. The driver behind this market is monetary gain, says Gutmann. The underground world of cyber criminals has its own sophisticated money laundering business, where funds are moved and laundered in many different ways, for example using compromised bank accounts, he says. There are also cashiers who will cash out and move the funds for you. E-mail addresses, zero-day exploits and credit card numbers are available for sale online. Credit card checks are easily done via Internet relay chat botnets — right down to the CVV number, the three digit number on the back of the card which is required as an extra check by some merchants. "This is more sophisticated than many merchants," says Gutmann.

Source: <http://computerworld.co.nz/news.nsf/scrt/F41324C51BB03DB2CC2572ED00011F7C>

9. *June 01, Computerworld* — **One year later: Five lessons learned from the VA data breach.**

It's been just over a year since the U.S. Department of Veterans Affairs (VA) disclosed that a laptop PC and external hard disk containing personal data on 26.5 million veterans and active-duty military personnel were stolen from the home of a VA employee. "Because of the sheer size of the VA breach, and because it was an issue that related to veterans, it really brought home the issue of security in a way that was not there prior" to the incident, said Geoff Gray, a lobbyist at the Cyber Security Industry Alliance. "If the question is, 'What rises to a level to really draw the attention of policymakers,' this one did," he said. Five lessons learned and steps taken in the wake of the data breach, according to analysts and vendors, include: greater focus on data encryption within government; stronger breach notification guidelines within agencies; more attention to data retention, classification and minimization; stronger remote access policies; and more authority for agency CIOs.

Source: [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9022678&intsrc=hm\\_list](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9022678&intsrc=hm_list)

[[Return to top](#)]

## **Transportation and Border Security Sector**

10. *June 04, United Press International* — **Landing gear fails during California landing.** No one was injured when a Southwest Airlines Boeing 737's nose gear collapsed during a rough landing at Oakland International Airport in California. Flight 3050 was diverted to Oakland International Sunday, June 3, after pilots reported trouble with the plane's landing gear, the San Francisco Chronicle reported Monday. Southwest spokesperson Beth Harbin said the 119 passengers and crewmembers were evacuated via the aircraft's inflatable slides and no injuries were reported. Ian Gregor, a spokesperson with the Federal Aviation Administration (FAA) in Los Angeles, said the pilot told air traffic controllers at the airport that the lights for the landing gear mechanisms under the wings and on the nose of the plane indicated they were working properly. The controllers gave the pilot visual confirmation that the landing gear was down before a landing was attempted. However, the landing gear under the nose collapsed upon touchdown. Southwest Airlines and the FAA are investigating the incident. The plane originally was heading from Sacramento to San Diego.  
Source: [http://www.upi.com/NewsTrack/Top\\_News/2007/06/04/landing\\_gear\\_fails\\_during\\_calif\\_landing/8719/](http://www.upi.com/NewsTrack/Top_News/2007/06/04/landing_gear_fails_during_calif_landing/8719/)
11. *June 04, United Press International* — **Plot to blow up airport highlights the vulnerability of U.S. aviation system's infrastructure.** Authorities say that the plot was broken up long before it was operational and insist that the fuel tanks at John F. Kennedy International Airport are secure. However, aviation security experts say such infrastructure represents a vulnerable "back door" to the nation's airports. "The back door to airports has always been an issue," John Raidt, an aviation security specialist for the 9/11 Commission, told United Press International. "You have trucks coming and going ... you have aviation fuel," said Raidt. The foiled plot highlighted the need the commission identified to build security in at all levels of airport planning and construction, he said. The Transportation Security Administration, the federal agency set up by the U.S. Congress in the wake of the September 11 attacks to take responsibility for aviation security, oversees perimeter and infrastructure security at airports. But the work of protecting them day-to-day rests with airport operators, and a government audit last year found enforcement efforts were patchy.  
Source: [http://www.upi.com/Security\\_Terrorism/Analysis/2007/06/04/analysis\\_jfk\\_plot\\_shows\\_back\\_door\\_risk/1038/](http://www.upi.com/Security_Terrorism/Analysis/2007/06/04/analysis_jfk_plot_shows_back_door_risk/1038/)
12. *June 03, ABC News (CA)* — **Explosion rocks California's Mojave Airport.** A large explosion at a storage facility at the Mojave Airport around noon Sunday, June 3, shook nearby buildings and closed the airspace above. It is believed no one was injured in the explosion, which took place in a facility that stores blasting agents and high-grade explosives primarily used in the mining and construction industries, according to Insp. Tony Diffenbaugh of the county fire department. An older-model aircraft caught fire as a result of the explosion, which sent large chunks of debris flying as far as a thousand feet from the facility. Airport officials, the environmental health department and several fire departments were on-scene investigating the explosion. The cause remains under investigation.  
Source: <http://www.turnto23.com/news/13435119/detail.html>
13. *June 02, Canadian Press* — **Canadian airports not planning security boost.** The terrorist plot targeting John F. Kennedy International Airport has some major Canadian airports taking notice, but two terrorism experts in Canada are casting doubt on whether the suspects had the

means or know-how to carry out such a devastating attack. U.S. federal authorities said Saturday, June 2, they had arrested three men — two from Guyana and one from Trinidad — and were seeking a fourth in Trinidad. Authorities said they were planning to destroy JFK airport and kill thousands of people by blowing up a jet fuel artery that runs through residential neighborhoods. The Port Authority of New York and New Jersey said JFK and the area's other airports remained at a heightened state of alert on Saturday. But a spokesperson for the Canadian Air Transport Security Authority said despite the U.S. plot, it's the status quo at Canadian airports. But officials at Canada's largest airport, Toronto's Pearson International, which served 31 million passengers last year, are taking note. Scott Armstrong, media relations manager for the Greater Toronto Airports Authority, said Saturday that anytime something happens that may affect an airport that's the size of Toronto's airport they'll take a look at procedures and protocols.

Source: <http://www.thestar.com/News/article/220924>

**14. *June 02, Fox23 News (NY)* — Bomb scare on Amtrak train in Schenectady, New York.**

Schenectady Police say an 84-year-old Philadelphia man is in Amtrak Police custody and will undergo a psychiatric evaluation after he allegedly threatened to blow up a passenger train on Saturday night, June 2. Investigators tell FOX23 News that State Police bomb-sniffing dogs didn't find any evidence of explosives on the section of the train where the man had been seated. Officials say the device the man displayed turned out to be a transistor radio. Schenectady Police Captain Pete Frisoni says the incident started at approximately 7:45 p.m. EDT on Saturday — about ten minutes after the train left Rensselaer. Frisoni says the man wouldn't tell investigators exactly why he made the threats but police believe he was upset because the train was running 25 minutes late. Officials separated the two cars in question from the rest of the train; the remaining cars traveled into the Schenectady train station where officials evacuated passengers. The passengers riding on the two cars along with the man who made the threats were put on a CDTA bus and then driven to the Schenectady station. Captain Frisoni said the Amtrak train was carrying 199 passengers and nine crewmembers.

Source: [http://www.fox23news.com/news/local/story.aspx?content\\_id=cc941d26-9f06-433e-b73f-a4dbc39903f](http://www.fox23news.com/news/local/story.aspx?content_id=cc941d26-9f06-433e-b73f-a4dbc39903f)

[[Return to top](#)]

## **Postal and Shipping Sector**

**15. *June 04, Associated Press* — Bomb intended for police found at post office.** A package containing an explosive device and addressed to the local police department was discovered in the West Plains, MO, post office and rendered safe, according to U.S. Postal Inspector Dan Taylor. A postal employee noticed the "suspicious package" addressed to the West Plains Police Department on Friday, June 2, and notified police. The Missouri Highway Patrol Bomb Unit was called in and rendered the package safe soon after X-raying the package and confirming that it contained an explosive device. A reward of \$100,000 has been issued by the Postal Service for information leading to the arrest and conviction of the suspect.

Source: <http://www.kctv5.com/Global/story.asp?S=6604847>

[[Return to top](#)]

## **Agriculture Sector**

16. *June 03, Stop Soybean Rust News* — **Asian soybean rust found on kudzu in Texas.** Asian soybean rust has overwintered in a known infected patch of kudzu under a bridge in Liberty County, Texas, officials report. It becomes the 23rd U.S. county or parish with rust this year. Texas officials said rust was found on kudzu under a bridge north of Dayton.  
Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=1041>
17. *May 31, Animal and Plant Health Inspection Service* — **USDA restricts ash nursery stock, other plant products from Canada.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) Thursday, May 31, published an interim rule establishing regulations to prohibit or restrict the importation of ash nursery stock and other propagative plant material from Canada to prevent the artificial spread of emerald ash borer (EAB), a destructive wood-boring insect that attacks and kills ash trees, into noninfested areas of the U.S. Plant health officials in the U.S. and Canada have been working cooperatively to establish a regulatory framework to address the risk of artificially spreading this plant pest between the two countries. APHIS is amending regulations in 7 CFR part 319, "Foreign Quarantine Notices," to restrict or prohibit EAB host material from Canada, including nursery stock, plants, other propagative plant material, ash logs and wood with bark that cannot be feasibly inspected, treated or handled to prevent the introduction of the pest. EAB, an insect indigenous to Asia, was first found in North America in ash trees in several counties in Michigan and a small area in Ontario, Canada. APHIS subsequently quarantined 13 counties in Michigan. The pest has since been found in Illinois, Indiana, Maryland and Ohio and quarantines have been established in those states as well.  
Source: <http://www.aphis.usda.gov/newsroom/content/2007/05/ashprodct.shtml>

[[Return to top](#)]

## **Food Sector**

18. *June 03, Food safety and Inspection Service* — **Ground beef recalled.** United Food Group, LLC, a Vernon, CA, establishment, is voluntarily recalling approximately 75,000 pounds of ground beef products because they may be contaminated with E. coli O157:H7, the U.S. Department of Agriculture's Food Safety and Inspection Service announced Sunday, June 3. The problem was discovered through sampling done by the California Department of Health Services and the Colorado Department of Health, in coordination with the U.S. Centers for Disease Control and Prevention, in the course of an investigation into illnesses. The ground beef products were produced on April 20 and were shipped to retail distribution centers in Arizona, California, Colorado, Oregon and Utah. E. coli O157:H7 is a potentially deadly bacterium that can cause bloody diarrhea and dehydration. The very young, seniors and persons with compromised immune systems are the most susceptible to foodborne illness.  
Source: [http://www.fsis.usda.gov/News\\_&\\_Events/Recall\\_025\\_2007\\_Releasse/index.asp](http://www.fsis.usda.gov/News_&_Events/Recall_025_2007_Releasse/index.asp)
19. *June 01, U.S. Food and Drug Administration* — **FDA advises consumers to avoid toothpaste from China.** The U.S. Food and Drug Administration (FDA) Friday, June 1, warned consumers to avoid using tubes of toothpaste labeled as made in China, and issued an import

alert to prevent toothpaste containing the poisonous chemical diethylene glycol (DEG) from entering the U.S. DEG is used in antifreeze and as a solvent. Out of an abundance of caution, FDA suggests that consumers throw away toothpaste with that labeling. FDA is concerned that these products may contain "diethylene glycol," also known as "diglycol" or "diglycol stearate." FDA is not aware of any U.S. reports of poisonings from toothpaste containing DEG. However, the agency is concerned about potential risks from chronic exposure to DEG and exposure to DEG in certain populations, such as children and individuals with kidney or liver disease. DEG in toothpaste has a low but meaningful risk of toxicity and injury to these populations. FDA has identified the following brands of toothpaste from China that contain DEG and are included in the import alert: Cooldent Fluoride; Cooldent Spearmint; Cooldent ICE; Dr. Cool, Everfresh Toothpaste; Superdent Toothpaste; Clean Rite Toothpaste; Oralmax Extreme; Oral Bright Fresh Spearmint Flavor; Bright Max Peppermint Flavor; ShiR Fresh Mint Fluoride Paste; DentaPro; DentaKleen; and DentaKleen Junior.

Source: <http://www.fda.gov/bbs/topics/NEWS/2007/NEW01646.html>

20. *June 01, BBC News* — **European Union urged to relax farm feed rules.** The European Union (EU) is currently funding research on the impacts of feeding animal carcasses to other farm animals. But the European Economic and Social Committee said this work had to be "stepped up" as the ban on meatmeal had caused a financial burden for farmers. The use of animal by-products in animal feed was halted in 2000 at the height of the United Kingdom's (UK) BSE crisis. BSE (Bovine Spongiform Encephalopathy) or "mad cow disease" was spread by the practice of feeding infected cattle remains to other cattle on farms. In the UK, thousands of cattle contracted the disease.

Source: <http://news.bbc.co.uk/1/hi/sci/tech/6711179.stm>

21. *May 31, Animal and Plant Health Inspection Service* — **Mexican state of Nayarit gains classical swine fever-free status.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is amending its regulations to add the Mexican state of Nayarit to the list of regions considered to be free of classical swine fever (CSF). APHIS conducted a thorough risk evaluation that determined the region is CSF free. Under this final rule, Nayarit must meet certain certification requirements in order to export live swine, pork and pork products to the U.S. and continue to ensure its freedom from CSF. Although Nayarit is considered CSF free, the state is located adjacent to regions that are still considered infected. In order to export to the U.S., Nayarit would have to certify the products' origin, move and process pork products in CSF-free zones and require that all processing facilities be inspected by the government of Mexico. Nayarit is not a major swine production area. In 2004, 34 commercial swine farms were located in Nayarit, with a population of 30,634 animals. This rulemaking is unlikely to have a significant effect on U.S. pork and pork products markets since Mexico is mainly an importer of U.S. pork.

Source: <http://www.aphis.usda.gov/newsroom/content/2007/05/nayaritcsf.shtml>

[[Return to top](#)]

## **Water Sector**

22. *June 01, U.S. Geological Survey* — **Record low streamflow for May in many Georgia rivers.** May was a dry month in Georgia bringing many of the State's rivers and streams to their

lowest levels ever recorded for the month. The U.S. Geological Survey has been monitoring and recording stream flow for more than 100 years at many locations throughout the State. The lowest May streamflow on record was recorded for 34 monitoring stations with at least 30 years of record in Georgia with many other rivers approaching record lows. Rivers across the state are experiencing moderate to severe hydrologic drought. This was the lowest May streamflow recorded in 115 years for the Oostanula River at the Resaca gage; 110 years for the Oconee River at the Milledgeville gage, and 98 years for the Flint River at the Albany gage. Streamflow was the lowest recorded for 50 years for any month for the Suwannee River at Fargo. Normally the lowest streamflows of the year occur in late summer, when water use demands are highest, and fall. If below average rainfall continues through the summer and fall, new record low flows are likely to occur in Georgia's rivers. With the conditions so dry this early in the year, it could create significant impacts to water supplies.

Source: <http://ga.water.usgs.gov/drought/may2007pressrelease.html>

[\[Return to top\]](#)

## **Public Health Sector**

**23. *June 02, Xinhua (China)* — Vietnam reports second bird flu patient.** A local man from Vietnam's northern Thai Nguyen province has been tested positive to bird flu virus strain H5N1, becoming the country's second bird flu patient since November 2005, Vietnam News Agency reported on Saturday, June 2. Quoting the Preventive Medicine Department under the Health Ministry, the report said the man from the province's Pho Yen district, who worked at a poultry slaughterhouse in Hanoi on May 14 and developed bird flu symptoms five days later, was admitted to the city-based Tropical Disease Hospital and now has to use a respirator. Late last month, the ministry confirmed that a 30-year-old man from Me Linh district, northern Vinh Phuc province became the country's latest bird flu patient after a 17-month absence of human infections. The man named Phung Minh Phuc, exhibiting bird flu symptoms on May 10 after having slaughtered chickens for a wedding party, is recovering well at the city-based Bach Mai Hospital. The Bach Mai Hospital received two men with bird flu symptoms on May 31 and June 1, one of them died, and the other, a 29-year-old policeman, who has taken part in culling infected fowls, is under treatment.

Source: [http://news.xinhuanet.com/english/2007-06/02/content\\_6188950.htm](http://news.xinhuanet.com/english/2007-06/02/content_6188950.htm)

**24. *June 01, Washington Post* — Release of microbe study spurs bioterror worries.** Researchers in Germany reported Thursday, May 31, that they had altered the DNA of a disease-causing bacterium to enable it to infect a species it cannot normally sicken — a double-edged advance that experts said could deepen scientists' understanding of human diseases but could also speed the development of novel bioterrorism agents. The change in infectiousness — the first of its kind ever engineered from scratch — poses no direct threat to human health, scientists said, because the microbe already causes a human disease: the food-borne illness called listeriosis. The change allows that microbe to sicken mice, a species it has no natural capacity to infect. Still, the work has biosecurity implications because it could, in theory, be applied in reverse, endowing a bacterium that causes a serious animal disease with an unprecedented ability to sicken people.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/31/AR2007053102159.html>

[\[Return to top\]](#)

## **Government Sector**

Nothing to report.

[\[Return to top\]](#)

## **Emergency Services Sector**

25. *June 03, Marion Chronicle–Tribune (IN)* — **Disaster drill in Indiana shows need for improvement.** Looking at the notes from the recent disaster drill in Grant County, IN, the number of items needing improvement outweigh the positives by a score of 19 to 8. Being critical of what went wrong that night is a step to solving the problems should a real disaster of that proportion arise. The aim of the drill was to push emergency systems in Grant County to the limit. Among the incidents that happened during the mock drill May 23, was a hostage situation with injured victims (in the end three people died, including the gunman); a two-vehicle wreck; a hospital emergency room besieged by patients; and a riot over medicine at a pharmacy. This was in the middle of a flu pandemic, so 30 percent of the personnel were out. One strength was how the agencies worked well together. The weaknesses centered around the areas of communication — with equipment, not people. It is best summed up on the notes in areas for "Areas for improvement:" in which it reads "Communication is a strength and a failure we need to work on. At times, people resorted to using cell phones because radios weren't effective."

Source: <http://www.chronicle-tribune.com/apps/pbcs.dll/article?AID=/20070603/OPINION02/706030302/1014/OPINION>

26. *June 03, Palo Alto Daily News (CA)* — **Emergency calls placed on hold.** For some San Francisco Peninsula residents, calling 911 from a cell phone during an emergency only to be told by a recorded voice to hold for the next available dispatcher can be an alarming experience. Sometimes the wait is brief, but other times it can stretch on for minutes, with the caller not knowing how long the wait will be. The problem is that in many areas, 911 calls from cell phones are automatically routed to the California Highway Patrol (CHP) dispatch center in Vallejo, which fields calls from all over the Bay Area. The CHP is hoping to resolve the situation by distributing the burden to local emergency dispatchers — and cities up and down the Peninsula are stepping up to accept the challenge. Relief might be on the way. Under California's Wireless E-9-1-1 Project, which was prompted by a Federal Communications Commission order aimed at enabling local jurisdictions to pick up their own cell phone 911 calls, agencies throughout the state are gradually converting to such systems.

Source: <http://www.paloaltodailynews.com/article/2007-6-3-scc-smc-911>

27. *June 02, Pittsburgh Tribune–Review* — **Pittsburgh's evacuation plans remain untested.** Authorities have plans to evacuate downtown Pittsburgh in the event of a disaster or terrorist attack. Yet, nearly six years after 9/11, those plans are inadequate and untested, they said Friday, June 1. One day after a bomb scare closed three Pittsburgh tunnels and halted rush-hour traffic for hours, Ray DeMichiei, deputy director of Pittsburgh's Emergency Management

Agency, said the city's Emergency Operations Center was partially activated Thursday, May 31, and that authorities were prepared to evacuate the city if necessary. But exactly how the plan would unfold, how long the evacuation would take, or even if it would work, is not known. Trooper Robin Mungo, a state police spokesperson, said an evacuation would be complicated by Pittsburgh's steep hills and wide rivers. "In most cases, you have to go over a bridge or through a tunnel (to enter or exit Downtown)," she said. "It's something authorities need to sit down and look at. Logistically, trying to evacuate the city — I don't know how well that would go over." Mungo said people should plan what to do in case of an emergency rather than wait for law enforcement's instructions.

Source: [http://www.pittsburghlive.com/x/pittsburghtrib/news/s\\_510659.html](http://www.pittsburghlive.com/x/pittsburghtrib/news/s_510659.html)

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

28. *June 04, IDG News Service* — **Stealthy attack method causes concern.** A new hacking method is causing concern for the lengths it goes to avoid detection by security software and researchers. The attack involves a Website that has been hacked to host malicious code, an increasingly common trap on the Internet. If a user visits one of the sites with an unpatched machine, it's possible that the computer can become automatically infected with code that can record keystrokes and steal financial data typed into forms. The new method, which uses special JavaScript coding, ensures that malicious code is only served up once to a computer that visits the rigged site, said security vendor Finjan. "These attacks represent a quantum leap for hackers in terms of their technological sophistication," according to the report. After a user visits the malicious Website, the hackers record the victim's IP address in a database. If the user goes to the site again, the malicious code will not be served, and a benign page will be served in its place.

The Finjan report can be downloaded after registration:

<https://www.finjan.com/Form.aspx?id=50&Openform=true&ObjId=443>

Source: [http://www.infoworld.com/article/07/06/04/Stealthy-attack\\_1.html](http://www.infoworld.com/article/07/06/04/Stealthy-attack_1.html)

29. *June 04, Newsfactor* — **McAfee study finds four percent of search results malicious.** "The State of Search Engine Safety," a recent study by McAfee's SiteAdvisor group, has some classic good news and bad news for Internet surfers. Using several automated techniques, the SiteAdvisor study determined that 4 percent of the query results offered by the major search engines lead to potentially dangerous Websites, and the total for sponsored links is nearly twice as high at 7 percent. The good news, however, is that the number of potentially dangerous search engine links has declined by roughly 20 percent from May 2006. The study was compiled by testing the links offered by the Internet's five largest search engines. McAfee concluded that AOL currently offers the safest search results, with Google second. Yahoo offered the highest number of potentially risky links in its search results. One of the more surprising results in the survey was the fact that it can be more dangerous to search for online music than it is for sexually explicit materials. The SiteAdvisor team found that 19.1 percent of the searches in the category of "digital music" led to risky sites, compared to just 9.4 percent for adult search terms.

Source: [http://business.newsfactor.com/story.xhtml?story\\_id=0100010V\\_ZY1S](http://business.newsfactor.com/story.xhtml?story_id=0100010V_ZY1S)

**30. June 04, VNUNet — Rogue security software on the rise.** Experts are warning of a sharp rise in the number of malware infections caused by rogue security programs. Trend Micro has reported a fivefold year-on-year increase in the use of such programs, which claim to clean a computer system but end up infecting users. Typically a user will visit a Webpage that includes a pop up warning that their computer is infected and offering a free trial of software to clean up the computer. Suspect software includes Winfixer, SpywareQuake, ErrorSafe, ErrorGuard, SpyShield, ApyAxe, SpywareNuker and, most recently, Spyhealer, DriverCleaner and SystemDoctor. "Rogue security programs are clearly on the rise, and users must demonstrate caution and always be alert when downloading software," said George Moore, threat researcher at Trend Micro.

Source: <http://www.vnunet.com/vnunet/news/2191329/rogue-security-software-rise>

**31. June 01, Sophos — Hack Attack: 9,500 new infected Webpages every day, reports Sophos.**

Sophos has revealed the most prevalent malware threats causing problems for computer users around the world during May 2007. The figures compiled by Sophos' global network of monitoring stations show that infected Webpages continue to pose a threat, affecting official government Websites as well as other legitimate pages. On average this month, Sophos uncovered 9,500 new infected Webpages daily — an increase of more than 1000 every day when compared to April. In total, 304,000 Webpages hosting malicious code were identified in May. The top ten list of Web-based malware threats in May 2007 is as follows: 1) Mal/frame; 2) JS/EnclFra; 3) Troj/Decdec; 4) Troj/Fujif; 5) Troj/lfradv; 6) VBS/Redlof; 7) Mal/ObfJS; 8) Troj/Psyme; 9) VBS/Roor; 10) VBS/Soraci.

Source: <http://www.sophos.com/pressoffice/news/articles/2007/06/toptenmay07.html>

### Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

## Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[[Return to top](#)]

## General Sector

Nothing to report.

[[Return to top](#)]

## **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.